# The Sign of an Elliptic Divisibility Sequence

JOSEPH H. SILVERMAN AND NELSON STEPHENS

ABSTRACT. An elliptic divisibility sequence (EDS) is a sequence of integers $(W_n)_{n\geq 0}$ generated by the nonlinear recursion satisfied by the division polyomials of an elliptic curve. We give a formula for the sign of $W_n$ for unbounded nonsingular EDS, a typical case being $\mathrm{Sign}(W_n) = (-1)^{\lfloor n\beta \rfloor}$ for an irrational number $\beta \in \mathbb{R}$. As an application, we show that the associated sequence of absolute values $(|W_n|)$ cannot be realized as the fixed point counting sequence of any abstract dynamical system.

## INTRODUCTION

A *divisibility sequence* is a sequence $(D_n)_{n\geq 0}$ of positive integers with the property that

$$m|n \Longrightarrow D_m|D_n.$$

Classical examples include sequences of the form $a^n - 1$ and various other linear recurrence sequences such as the Fibonacci sequence. See [1] for a complete classification of divisibility sequences arising from linear recurrences.

There are also natural divisibility sequences associated to nonlinear recurrence relations. The most famous such relation comes from the recursion formula for division polynomials on an elliptic curve.

**Definition 1.** An *elliptic divisibility sequence* (abbreviated EDS) is a divisibility sequence $W_0, W_1, W_2, \ldots$ that satisfies the formula

$$W_{m+n} \cdot W_{m-n} = W_{m+1} \cdot W_{m-1} \cdot W_n^2 - W_{n+1} \cdot W_{n-1} \cdot W_m^2 \qquad \text{for all } m \geq n \geq 1. \quad (1)$$

Note that the definition forces $W_0 = 0$ (put $m = n$) and, except in some degenerate cases, $W_1 = \pm 1$ (put $n = 1$). It is also possible to use the recursion (1) to extend the EDS backwards to negative indices, leading to the identity $W_{-n} = -W_n$.

*Date*: February 2004.
1991 *Mathematics Subject Classification.* Primary: 11D61; Secondary: 11G35.
*Key words and phrases.* elliptic divisibility sequence, elliptic curve, realizable sequence.

The arithmetic properties of elliptic divisibility sequences were first studied in detail by Morgan Ward [15, 16]. (See also [2, 3, 4, 6, 7, 9, 13].) Ward describes a number of degenerate cases for EDS and shows that all other EDS are associated in a precise way to a pair $(E, P)$ consisting of an elliptic curve $E/\mathbb{Q}$ and a point $P \in E(\mathbb{Q})$. These nondegenerate EDS are called *nonsingular*. (See Definition 2 for details.)

*Example* 1. The simplest (unbounded) nonsingular elliptic divisibility sequence is the sequence

$$\begin{aligned} &1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, 129, -314, \\ &\qquad\qquad -65, 1529, -3689, -8209, -16264, \ldots \end{aligned} \tag{2}$$

See Section 5 for further examples.

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation and let $P \in E(\mathbb{Q})$ be a nontorsion point. For each $n \geq 1$, we can write the $x$-coordinate of $nP$ in lowest terms as $x_{nP} = A_{nP}/D_{nP}^2$. It is not hard to prove that $(D_{nP})$ is a divisibility sequence, and as shown by Shipsey [9], it frequently turns out that $(D_{nP})$ is an elliptic divisibility sequence, i.e., it satisfies the recursion (1), provided that each $D_{nP}$ is chosen with the correct sign. See Section 3 for further details of this connection.

Thus *a priori*, the geometric construction of "elliptic divisibility sequences" via rational points on elliptic curves yields sequences $(D_{nP})$ of positive integers, while the algebraic construction via the recursion (1) yields sequences $(W_n)$ of signed integers. It is thus of interest to gain some understanding of how the signs of the terms of an EDS vary. Our first main result answers this question.

**Theorem 1.** *Let $(W_n)$ be an unbounded nonsingular elliptic divisibility sequence. Then possibly after replacing $(W_n)$ by the related sequence $\big((-1)^{n-1}W_n\big)$, there is an irrational number $\beta \in \mathbb{R}$ so that the sign of $W_n$ is given by one of the following formulas:*

$$\operatorname{Sign}(W_n) = (-1)^{\lfloor n\beta \rfloor} \quad \textit{for all } n.$$

$$\operatorname{Sign}(W_n) = \begin{cases} (-1)^{\lfloor n\beta \rfloor + n/2} & \textit{if } n \textit{ is even}, \\ (-1)^{(n-1)/2} & \textit{if } n \textit{ is odd}. \end{cases}$$

*(Here $\lfloor t \rfloor$ denotes the greatest integer in $t$.)*

We will prove a more precise theorem in which we use the parametrization of the associated elliptic curve as a real Lie group to describe the number $\beta$ and to determine which formula to use. See Theorem 4 for details.

Our second main result concerns the realizability of an EDS. In general, a sequence $(U_n)$ of positive integers is called *realizable* if there exists a set $X$ and a function $T : X \to X$ so that

$$U_n = \#\{x \in X : T^n(x) = x\} \qquad \text{for all } n \geq 1.$$

Thus realizable sequences are those arising from the theory of (abstract) dynamical systems. It is clear that an EDS cannot itself be realizable, since an EDS always has both positive and negative terms. Our second main result shows that the absolute values of the terms in an EDS are also not realizable.

**Theorem 2.** *Let $(W_n)$ be an unbounded nonsingular elliptic divisibility sequence. Then the associated positive sequence $(|W_n|)$ is not realizable.*

## 1. Preliminaries on elliptic divisibility sequences

A divisibility sequence $(D_n)$ is called *normalized* if $D_0 = 0$ and $D_1 = 1$. Notice that $D_n | D_0$, so if $D_0 \neq 0$, then $D_n$ is bounded. Further, since $D_1 | D_n$ for all $n \geq 1$, a divisibility sequence may be normalized by replacing $D_n$ with $D_n/D_1$. We will assume henceforth that all of our elliptic divisibility sequences are normalized.

An elliptic divisibility sequence $(W_n)$ is required to satisfy the recursion (1) for all $m \geq n \geq 1$. It is not hard to show that it suffices that $(W_n)$ satisfy the two relations

$$W_{2n+1} = W_{n+2}W_n^3 - W_{n-1}W_{n+1}^3, \tag{3}$$

$$W_{2n}W_2 = W_n\left(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2\right). \tag{4}$$

In particular, an EDS is determined by the values of $W_2, W_3, W_4$. Further, a triple $W_2, W_3, W_4$ with $W_2W_3 \neq 0$ gives an EDS if and only if $W_2 | W_4$. (See [15].)

We observe that if $(W_n)$ is an EDS, then $\left((-1)^{n-1}W_n\right)$ is also an EDS. We call $\left((-1)^{n-1}W_n\right)$ the *inverse EDS* to $(W_n)$, since in Ward's characterization (see Theorem 3) of EDS via elliptic functions, it corresponds to replacing the generating point $z$ by its additive inverse $-z$.

The elliptic divisibility sequences that are associated to elliptic curves are characterized by the following property.

**Definition 2.** The *discriminant* of an elliptic divisibility sequence sequence $(W_n)$ is defined by the formula

$$\begin{aligned}\operatorname{Disc}(W) = W_4W_2^{15} - W_3^3W_2^{12} + 3W_4^2W_2^{10} - 20W_4W_3^3W_2^7 \\ + 3W_4^3W_2^5 + 16W_3^6W_2^4 + 8W_4^2W_3^3W_2^2 + W_4^4.\end{aligned} \tag{5}$$

The elliptic divisibility sequence $(W_n)$ is said to be *nonsingular* if

$$W_2 \neq 0, \qquad W_3 \neq 0, \qquad \text{and} \qquad \operatorname{Disc}(W) \neq 0.$$

(Cf. Ward [15, equation (19.3)].)

See [2, 3, 4, 6, 7, 9, 13, 15, 16] for additional material on elliptic divisibility sequences. Ward proves that nonsingular elliptic divisibility sequences arise as values of the division polynomials of an elliptic curve. The complicated expression (5) defining $\operatorname{Disc}(W)$ is (essentially) the discriminant of the elliptic curve associated to the sequence $(W_n)$. See [15] for details and formulas, some of which are recalled in Appendix A. We also note that Ward gives a complete characterization of all singular EDS.

## 2. Elliptic divisibility sequences and elliptic functions

We recall Ward's fundamental result relating EDS to values of elliptic functions.

**Theorem 3.** *Let $(W_n)$ be a nonsingular elliptic divisibility sequence. Then there is a lattice $L \subset \mathbb{C}$ and complex number $z \in \mathbb{C}$ such that*

$$W_n = \frac{\sigma(nz, L)}{\sigma(z, L)^{n^2}} \qquad \text{for all } n \geq 1,$$

*where $\sigma(z, L)$ is the Weierstrass $\sigma$-function associated to the lattice $L$.*

*Further, the modular invariants $g_2(L)$ and $g_3(L)$ associated to the lattice $L$ and the Weierstrass values $\wp(z, L)$ and $\wp'(z, L)$ associated to the point $z$ on the elliptic curve $\mathbb{C}/L$ are in the field $\mathbb{Q}(W_2, W_3, W_4)$. In other words $g_2(L), g_3(L), \wp(z, L), \wp'(z, L)$ are all defined over the same field as the terms of the sequence $(W_n)$.*

*Proof.* See Ward [15, Theorems 12.1 and 19.1]. The rational expressions for $g_2$ and $g_3$ in $\mathbb{Q}(W_2, W_3, W_4)$ are given by [15, equations 13.6 and 13.7], while the rational expressions for $\wp(z, L)$ and $\wp'(z, L)$ are given by [15, equations 13.5 and 13.1]. For the convenience of the reader, we have reproduced these formulas in Appendix A

Ward also shows [15, Theorem 22.1] that up to equivalence, a singular sequence is either the trivial sequence $W_n = n$ or a Lucas sequence $W_n = \frac{a^n - b^n}{a - b}$. The latter may be viewed as arising from the degeneration of the $\sigma$-function to a trigonometric function. $\square$

## 3. Elliptic divisibility sequences and elliptic curves

There is a natural way to attach a divisibility sequence to any (non-torsion) rational point on an elliptic curve. (See [10, 11] for basic

properties of elliptic curves.) Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{6}$$

A nonzero rational point $P \in E(\mathbb{Q})$ can be written in the form

$$P = (x_P, y_P) = \left(\frac{A_P}{D_P^2}, \frac{B_P}{D_P^3}\right) \quad \text{with } \gcd(A_P, D_P) = \gcd(B_P, D_P) = 1.$$

Assume now that $P \in E(\mathbb{Q})$ is a nontorsion point. It is not hard to show that the sequence

$$\{D_{nP} : n = 1, 2, 3, \dots\}$$

is a divisibility sequence.

Further, it is often the case that $(D_{nP})$ is an elliptic divisibility sequence, with one important caveat, namely we must choose the signs correctly. For example, suppose that after moving $P$ to $(0, 0)$, there is a Weierstrass equation for the curve $E$ of the form

$$\begin{aligned} E : y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x \\ &\qquad \text{with } a_1, a_2, a_3, a_4 \in \mathbb{Z} \text{ and } \gcd(a_3, a_4) = 1. \end{aligned} \tag{7}$$

There is always some multiple $mP$ for $P$ for which this can be accomplished. More precisely, this is possible if and only if $P$ has everywhere nonsingular reduction on the Néron model of $E$ over $\operatorname{Spec}(\mathbb{Z})$.

Now define a sequence $W_n$ by setting

$$W_1 = 1, \qquad W_2 = a_3, \qquad |W_n| = |D_{nP}| \quad \text{for } n \geq 2,$$

and choosing the subsequent signs of $W_n$ by the rule

$$\operatorname{Sign}(W_{n-2}W_n) = -\operatorname{Sign}(A_{(n-1)P}) \qquad \text{for } n \geq 3.$$

Shipsey [9] shows that the sequence $(W_n)$ is an EDS.

However, if $P \in E(\mathbb{Q})$ is singular modulo some prime, then it may not be possible to assign signs to $\{\pm D_{nP}\}$ in order to make it into an EDS. For example, Shipsey [9] (see also [4, §10.3]) shows that the point $P = (0, 0)$ on the curve $E : y^2 + 27y = x^3 + 28x^2 + 27x$ is not associated to an EDS. The point $P$ is a singular point on $E$ modulo 3. The point $P' = (-1, 0) = 3P \in E(\mathbb{Q})$ is nonsingular modulo every prime, so $P'$ does give an EDS.

Conversely, Shipsey [9] shows that if $(V_n)$ is an EDS, then there is an ellliptic curve $E/\mathbb{Q}$ of the form (7) and an integer $k \geq 1$ so that the point $P = (0, 0) \in E(\mathbb{Q})$ gives a sequence $(W_n)$ as described above (i.e., with $|W_n| = D_{nP}$) such that $W_n = V_{nk}/V_k$ for all $n \geq 1$. For example, the EDS beginning $[1, 1, 3, 1, \dots]$ comes from the point $P = (0, 0)$ on the curve $E : y^2 + 27y = x^3 + 28x^2 + 27x$ and the value $k = 3$.

*Remark* 1. Divisibility sequences of the form $D_n = a^n - 1$ may be viewed as the values of the $n^{\text{th}}$ division polynomial $X^n - 1$ of the multiplicative group $\mathbb{G}_m$. The same is true of divisibility sequences arising from many other linear recurrences, although one must either use a twisted version of $\mathbb{G}_m$ or work in a quadratic field. Replacing $\mathbb{G}_m$ with an elliptic curve naturally leads to the theory of elliptic divisibility sequences. More generally, one can create divisibility sequences associated to rational points on any algebraic group, see [12] for details.

## 4. The sign of an elliptic divisibility sequence

To ease notation, for any real number $x$, we define the parity of $x$ by

$$\operatorname{Sign}(x) = (-1)^{\operatorname{Parity}(x)} \qquad \text{with } \operatorname{Parity}(x) \in \mathbb{Z}/2\mathbb{Z}.$$

**Theorem 4.** *Let $(W_n)$ be an unbounded nonsingular elliptic divisibility sequence. Then possibly after replacing $(W_n)$ by its inverse sequence $\big((-1)^{n-1}W_n\big)$, there is an irrational number $\beta \in \mathbb{R}$ so that the parity of $W_n$ is given by one of the following formulas:*

$$\operatorname{Parity}(W_n) \equiv \lfloor n\beta \rfloor \pmod 2 \quad \textit{for all } n. \tag{8}$$

$$\operatorname{Parity}(W_n) \equiv \begin{cases} \lfloor n\beta \rfloor + \frac{n}{2} \pmod 2 & \textit{if } n \textit{ is even,} \\ \frac{n-1}{2} \pmod 2 & \textit{if } n \textit{ is odd.} \end{cases} \tag{9}$$

*More precisely, use Theorem 3 to associate to $(W_n)$ an elliptic curve $E/\mathbb{R}$ and and point $P \in E(\mathbb{R})$. Fix an $\mathbb{R}$-isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ with $q \in \mathbb{R}$ and $|q| < 1$. Let $P \leftrightarrow u$, where $u$ is normalized to satisfy $q^2 < u < 1$ if $q < 0$ and $|q| < |u| < 1$ otherwise. Then the formula for the parity of $W_n$ and the value of $\beta$ are given in the following table:*

| $q$ | $u$ | *Formula* | $\beta$ | $E(\mathbb{R})$ | $P$ |
|---|---|---|---|---|---|
| $q > 0$ | $u > 0$ | (8) | $\log_q(u)$ | *Disconnected* | *Identity component* |
| $q > 0$ | $u < 0$ | (9) | $\log_q(\lvert u\rvert)$ | *Disconnected* | *Nonidentity component* |
| $q < 0$ | | (8) | $\frac{1}{2}\log_{\lvert q\rvert}(u)$ | *Connected* | |

*Remark* 2. Theorem 4 is true for any unbounded sequence of *real numbers* $(W_n)$ satisfying the recursion (1), subject to the nonsingularity condition (2).

*Proof of Theorem 4.* The proof of Theorem 4 relies on Ward's fundamental result (Theorem 3) relating ellipitic divisibility sequences to the values of elliptic functions. Let $(W_n)$ be an unbounded nonsingular elliptic divisibility sequence, and choose a lattice $L$ and complex

number $z$ as in Theorem 3 so that

$$W_n = \frac{\sigma(nz, L)}{\sigma(z, L)^{n^2}}. \tag{10}$$

Let $E$ be the associated elliptic curve

$$E : Y^2 = 4X^3 - g_2(L)X - g_3(L)$$

and $P = \bigl(\wp(z, L), \wp'(z, L)\bigr)$ the associated point on $E$. Theorem 3 tells us that $E$ is defined over $\mathbb{Q}$ (i.e., $g_2(L), g_3(L) \in \mathbb{Q}$) and that $P \in E(\mathbb{Q})$. In particular, $E$ and $P$ are defined over $\mathbb{R}$. Then [11, V.2.3(b)] says that there exists a (unique) $q \in \mathbb{R}$ with $0 < |q| < 1$ such that there is an $\mathbb{R}$-isomorphism

$$\psi : \frac{\mathbb{C}^*}{q^{\mathbb{Z}}} \xrightarrow{\ \sim\ } E(\mathbb{C}).$$

(See [11, V.1.1] for explicit power series defining $\psi$.) The fact that $\psi$ is defined over $\mathbb{R}$ means that it gives an isomorphism $\psi : \mathbb{R}^*/q^{\mathbb{Z}} \to E(\mathbb{R})$, so the fact that $P \in E(\mathbb{R})$ implies that $\psi^{-1}(P) \in \mathbb{R}^*/q^{\mathbb{Z}}$. Let $u \in \mathbb{R}^*$ be a representative for $\psi^{-1}(P)$.

Write $u = e^{2\pi i\alpha}$ with (say) $\alpha \in i\mathbb{R}$ if $u > 0$ and $\alpha \in \frac{1}{2} + i\mathbb{R}$ if $u < 0$. Then the $\sigma$-function on $\mathbb{C}^*/q^{\mathbb{Z}}$ is given by the formula [11, V.1.3]

$$\sigma(u, q) = -\frac{1}{2\pi i} e^{\frac{1}{2}\eta\alpha^2 - \pi i\alpha}\theta(u, q) \quad \text{with}$$
$$\theta(u, q) = (1 - u) \prod_{m \geq 1} \frac{(1 - q^m u)(1 - q^m u^{-1})}{(1 - q^m)^2}. \tag{11}$$

Here $\eta$ is a quasiperiod, but its value will not concern us, since it disappears when we substitute (11) into (10). However, it is important to observe that the $\sigma$-function in formula (10) and the $\sigma$-function defined by the formula (11) may only be constant multiples of one another, since $\sigma(z, L)$ has weight one (i.e., $\sigma(cz, cL) = c\sigma(z, L)$). Hence when we substitute (11) into (10), we obtain

$$W_n = \gamma^{n^2-1} u^{(n^2-n)/2} \frac{\theta(u^n, q)}{\theta(u, q)^{n^2}} \tag{12}$$

for some $\gamma \in \mathbb{C}^*$. However, since $u$, $q$, and $W_n$ are all in $\mathbb{R}$, taking $n = 2$ and $n = 3$ shows that $\gamma^3 \in \mathbb{R}$ and $\gamma^8 \in \mathbb{R}$, so $\gamma \in \mathbb{R}$.

We observe that since $n^2 - 1 \equiv n - 1 \pmod 2$ for all $n \in \mathbb{Z}$, the effect of a negative $\gamma$ is simply to replace an EDS starting $[1, a, b, c]$ with the asociated inverse sequence starting $[1, -a, b, -c]$. Hence without loss of generality, we may assume that $\gamma > 0$.

Since $|q| < 1$, we see that $1 - q^m > 0$ for all $m \geq 1$. Thus in computing the sign of $W_n$ using (12), we may discard the $(1 - q^m)^2$

factors appearing in the product expansion (11) for $\theta(u,q)$. We now consider several cases, depending on the sign of $q$ and $u$.

**Case I**: $1 > q > 0$ and $u > 0$.
Geometrically, this is the case that $\mathbb{R}^*/q^{\mathbb{Z}}$ has two components and the point $P = \psi(u)$ is on the identity component. The value of the righthand side of (12) is invariant under $u \to q^{\pm 1}u$, so we may choose $u$ to satisfy $q < u < 1$. Then

$$1 - u > 0 \qquad \text{and} \qquad 1 - q^m u^{\pm 1} > 0 \quad \text{for all } m \geq 1,$$

so $\theta(u,q) \geq 0$. We next do a similar analysis for $\theta(u^n,q)$. The assumption $0 < q < u < 1$ and the fact that we take $n \geq 1$ implies that

$$1 - q^m u^n > 0 \qquad \text{for all } m \geq 1.$$

So the only sign ambiguity in $\theta(u^n,q)$ comes from the factors of the form $1 - q^m u^{-n}$. We have

$$1 - q^m u^{-n} < 0 \iff u^n < q^m \iff n \log_q(u) > m.$$

Hence there are $\lfloor n \log_q(u) \rfloor$ negative signs. This proves that

$$\operatorname{Parity}(W_n) \equiv \operatorname{Parity}(\theta(u^n,q)) \equiv \lfloor n \log_q(u) \rfloor \pmod 2,$$

which is the desired result (8) with the explicit value $\beta = \log_q(u)$.

**Case II**: $1 > q > 0$ and $u < 0$.
Geometrically, we are again in the case that $\mathbb{R}^*/q^{\mathbb{Z}}$ has two components, but now the point $u$ is on the nonidentity component. We may choose $u$ to satisfy $q < |u| < 1$, and then as in Case I, we see that $\theta(u,q) > 0$ and that all factors $1 - q^m u^n$ are positive. Further, since $u < 0$ and $q > 0$, it is clear that $1 - q^m u^{-n} > 0$ for all odd values of $n$. Thus if $n$ is odd, we also have $\theta(u^n,q) > 0$.

Suppose now that $n$ is even. Then

$$1 - q^m u^{-n} < 0 \iff |u|^n < q^m \iff n \log_q(|u|) > m.$$

Hence there are $\lfloor n \log_q(|u|) \rfloor$ negative signs, so

$$\operatorname{Parity}(\theta(u^n,q)) \equiv \lfloor n \log_q(|u|) \rfloor \pmod 2 \qquad \text{when } n \text{ is even.}$$

Finally, since $u < 0$, we observe that

$$\operatorname{Parity}\left(u^{(n^2-n)/2}\right) \equiv \frac{n^2-n}{2} \equiv \begin{cases} n/2 \pmod 2 & \text{if } n \text{ is even,} \\ (n-1)/2 \pmod 2 & \text{if } n \text{ is odd.} \end{cases}$$

Combining these results and substituting into (12) yields the desired result (9) with the explicit value $\beta = \log_q(u)$.

**Case III**: $q < 0$.
Geometrically, this is the case that the curve $\mathbb{R}^*/q^{\mathbb{Z}}$ is connected. Replacing $u$ by $q^k u$ for an appropriate $k \in \mathbb{Z}$, we may assume that

$$u > 0 \qquad \text{and} \qquad q^2 < u < 1.$$

Consider first the factors $1 - q^m u^{\pm 1}$ of $\theta(u, q)$. For our choice of $u$, we have

$$1 - q^m u^{\pm 1} > 1 - |q|^{m-2},$$

so $1 - q^m u^{\pm 1}$ is positive except possibly when $m = 1$. However, when $m = 1$, it is also positive, since $q < 0$ and $u > 0$. Hence $\theta(u, q) > 0$.

Next we look at the factors of $\theta(u^n, q)$. The factors $1 - q^m u^n$ are positive, since $|q| < 1$ and $u < 1$. Further, the factors $1 - q^m u^{-n}$ with $m$ odd are also positive, since $q < 0$ and $u > 0$. Suppose now that $m$ is even. Then

$$1 - q^m u^{-n} < 0 \iff u^n < |q|^m \iff n \log_{|q|}(u) > m.$$

Thus we get one negative factor in $\theta(u^n, q)$ for each even integer smaller than $n \log_{|q|}(u)$, so

$$\operatorname{Parity}(W_n) \equiv \operatorname{Parity}(\theta(u^n, q)) \equiv \left\lfloor \frac{1}{2} \log_{|q|}(u) \right\rfloor \pmod{2}.$$

This yields the desired result (8) with the explicit value $\beta = \frac{1}{2} \log_{|q|}(u)$, which completes the proof of Theorem 4. $\square$

## 5. Numerical examples

We give some examples of elliptic divisibility sequences that illustrate the various cases of Theorem 4.

*Example* 2. The elliptic divisibility sequence starting $[1, 1, -1, 1]$ is

$$1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, 129, -314, \\ -65, 1529, -3689, -8209, -16264, \ldots \quad (13)$$

This is the elliptic divisibility sequence associated to the elliptic curve $E : y^2 + y = x^3 - x$ of conductor 37 and the point $P = (0, 0) \in E(\mathbb{Q})$. The point $P$ has canonical height $\hat{h}(P) \approx 0.0256$. Among elliptic curves over $\mathbb{Q}$ of positive rank, this is the one of smallest conductor. So in some sense (13) is the "smallest" or "simplest" possible elliptic divisibility sequence. The authors of [4] liken it to the simplest linear divisibility sequence $2^n - 1$.

There is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ with $P \leftrightarrow u$, where

$$q = 0.0004654203923\ldots \qquad \text{and} \qquad u = -0.09230562888\ldots.$$

Thus $E(\mathbb{R})$ is disconnected and $P$ is on the nonidentity component, so Theorem 4 says that

$$\mathrm{Parity}(W_n) \equiv \begin{cases} \lfloor n\beta \rfloor + \frac{n}{2} + 1 & \text{if } n \text{ is even,} \\ \frac{n-1}{2} & \text{if } n \text{ is odd,} \end{cases}$$
$$\text{with } \beta = \log_q(|u|) = 0.310541358720\ldots.$$

Notice that we have added one for the even values of $n$, since Theorem 4 gives the sign of either the sequence $(W_n)$ or the sequence $((-1)^{n-1}W_n)$.

*Example* 3. The elliptic divisibility sequence starting $[1, 1, 1, -1]$ is

$$1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191, -197, 1018,$$
$$2681, 8191, -5841, -81289, -261080, \ldots \quad (14)$$

This is the elliptic divisibility sequence associated to the elliptic curve $E : y^2 + y = x^3 + x^2$ of conductor 43 and the point $P = (0, 0) \in E(\mathbb{Q})$. The point $P$ has canonical height $\hat{h}(P) \approx 0.0314$.

There is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ with $P \leftrightarrow u$, where

$$q = -0.001833413287\ldots \qquad \text{and} \qquad u = 0.02931619135\ldots.$$

Thus $E(\mathbb{R})$ is connected, so Theorem 4 says that

$$\mathrm{Parity}(W_n) \equiv \lfloor n\beta \rfloor \qquad \text{with } \beta = \frac{1}{2}\log_q(|u|) = 0.2800581462\ldots.$$

*Example* 4. The elliptic divisibility sequence starting $[1, 1, 2, 1]$ is

$$1, 1, 2, 1, -7, -16, -57, -113, 670, 3983, 23647, 140576, -833503,$$
$$-14871471, -147165662, -2273917871, 11396432249, 808162720720,$$
$$14252325989831, 503020937289311, \ldots \quad (15)$$

This is the elliptic divisibility sequence associated to the elliptic curve $E : y^2 + xy = x^3 - x^2 - x + 1$ of conductor 58 and the point $P = (1, 0) \in E(\mathbb{Q})$. The point $P$ has canonical height $\hat{h}(P) \approx 0.0848$. The reason that (15) grows so much faster than (13) or (14) is due to the larger height of $P$. One can show that (roughly) $|W_n| \approx \exp\left(\frac{1}{2}n^2\hat{h}(P)\right)$.

There is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ with $P \leftrightarrow u$, where

$$q = -0.0004429838967\ldots \qquad \text{and} \qquad u = 0.02529988312\ldots.$$

Thus as in the previous example, $E(\mathbb{R})$ is connected and

$$\mathrm{Parity}(W_n) \equiv \lfloor n\beta \rfloor \qquad \text{with } \beta = \frac{1}{2}\log_q(|u|) = 0.2380838117\ldots.$$

*Example* 5. The elliptic divisibility sequence starting $[1, 1, 1, 2]$ is

$$\begin{aligned} 1, 1, 1, 2, 1, -3, -7, -8, -25, -37, 47, 318, 559, 2023, 7039, -496,& \\ -90431, -314775, -1139599, -8007614, \dots& \quad (16) \end{aligned}$$

This is the elliptic divisibility sequence associated to the elliptic curve $E : y^2 + xy = x^3 - 2x + 1$ of conductor 61 and the point $P = (1, 0) \in E(\mathbb{Q})$. The point $P$ has canonical height $\hat{h}(P) \approx 0.0396$. We have $q = -0.00006372107969$ and $u = 0.02660268122$, so again $E(\mathbb{R})$ is connected and

$$\text{Parity}(W_n) \equiv \lfloor n\beta \rfloor \qquad \text{with } \beta = \frac{1}{2}\log_q(|u|) = 0.1877002949\dots.$$

*Example* 6. The elliptic divisibility sequence starting $[1, 2, 2, -2]$ is

$$\begin{aligned} 1, 2, 2, -2, -24, -100, -176, 1552, 28448, 248448, 433024,& \\ -47795200, -1682842624, -30121422848, 218738737152, \dots& \quad (17) \end{aligned}$$

This is the elliptic divisibility sequence associated to the elliptic curve $E : y^2 + xy + y = x^3 + x^2 - 416x + 3009$ of conductor 710 and the point $P = (21, 53) \in E(\mathbb{Q})$. The point $P$ has canonical height $\hat{h}(P) \approx 0.08372$. However, if we write $x(nP) = A_n/D_n^2$, then it is not true that $|W_n| = D_n$. The difficulty arises because $P$ is singular modulo 2. One can check that $W_n/D_n = \pm 2^k$ for all $n$.

There is an isomorphism $E(\mathbb{R}) \cong \mathbb{R}^*/q^{\mathbb{Z}}$ with $P \leftrightarrow u$, where

$$q = 0.00002987174044\dots \qquad \text{and} \qquad u = 0.0004951251683\dots.$$

Thus $E(\mathbb{R})$ is disconnected and $P$ is on the identity component, so Theorem 4 says that

$$\text{Parity}(W_n) \equiv \lfloor n\beta \rfloor + (n-1) \qquad \text{with } \beta = \log_q(u) = 0.7304917812\dots.$$

Notice that as in Example 2, the theorem gives the sign of $(-1)^{n-1}W_n$, so we needed to adjust by $n - 1$.

## 6. Elliptic divisibility sequences and realizability

A sequence is said to be realizable if it gives the number of fixed points of the iterates of some map. As an application of Theorem 4, we show in this section that the absolute value of an elliptic divisibility sequence is not realizable. See [4, Section 11.2] and [5] for further information about realizability.

**Definition 3.** Let $(U_n)_{n\geq 1}$ be a sequence of nonnegative integers. We say that $(U_n)$ is *realizable* if there exists a set $X$ and a function $\phi : X \to X$ with the property that

$$U_n = \#\{x \in X : T^n(x) = x\} \qquad \text{for all } n \geq 1.$$

*Remark* 3. It is clear from Theorem 4 that an EDS cannot be realizable, since $(W_n)$ will always contain terms that are negative. It turns out that the sequence of absolute values $(|W_n|)$ is also not realizable, but the proof, which we give below, is less direct.

*Remark* 4. There are many *linear* recurrence sequences that are known to be realizable. A simple example is the Lucas sequence $L_{n+2} = L_{n+1} + L_n$ with initial terms $L_1 = 1$ and $L_2 = 3$. Linear recurrence sequences grow linearly exponentially, i.e., $\log|L_n| = O(n)$. Elliptic divisibility sequences generally grow much more rapidly, namely $\log|W_n| = O(n^2)$. At the present time, there are no realizable sequences known that grow quadratic exponentially. Elliptic divisibility sequences, with their added structure, are thus a natural place to search for rapidly growing realizable sequences. The main result in this section shows that unfortunately the EDS recursion never gives a realizable sequence.

There is an elementary combinatorial characterization of realizable sequences. We recall that the Dirichlet product of two arithmetic functions $f$ and $g$ is defined by the formula

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

**Lemma 5.** *A sequence $(U_n)$ of positive integers is realizable if and only*

$$(U * \mu)(n) \geq 0 \qquad \text{for all } n \geq 1, \text{ and} \tag{18}$$

$$(U * \mu)(n) \equiv 0 \pmod{n} \qquad \text{for all } n \geq 1. \tag{19}$$

*(Here $\mu(n)$ is the Möbius function.)*

*Proof.* See [4, Lemma 11.3]. $\square$

*Remark* 5. Applying (19) to a prime power $p^k$ shows that a realizable sequence necessarily satisfies

$$U_{p^k} \cong U_{p^{k-1}} \pmod{p^k} \qquad \text{for all } k \geq 1. \tag{20}$$

In particular, the limit

$$\lim_{k\to\infty} U_{p^k} \in \mathbb{Z}_p \qquad \text{exists in } \mathbb{Z}_p.$$

It would interesting to give a dynamical interpretation to this limit. For the proof of the nonrealizibility of an EDS, we will only require the very special case of (20) which asserts that $U_{2^k} \equiv U_{2^{k-1}} \pmod 4$ for all $k \geq 2$.

The following lemma provides a (weak) EDS counterpart to the $p$-adic coherence (20) of a realizable sequence, at least for the prime $p = 2$.

**Lemma 6.** *Let $(W_n)$ be an unbounded EDS, and assume that $W_2$ and $W_4$ are odd. Then $W_{2^k}$ is odd for all $k \geq 0$, and for any fixed power $2^e$, the sequence $W_{2^k} \bmod 2^e$ is eventually periodic, i.e., there are integers $r, K > 0$ so that*

$$W_{2^{r+k}} \equiv W_{2^k} \pmod{2^e} \qquad \text{for all } k \geq K.$$

*Remark* 6. Lemma 6 says that the sequence $(W_{2^k} \bmod 2^e)_{k\geq 0}$ is eventually periodic, and an adaptation of the proof of Lemma 6 gives a similar result with 2 replaced by other primes. This suggests that something stronger might be true.

*Question.* Let $(W_n)$ be an unbounded EDS. Does there exist an exponent $e \geq 1$ so that for each $0 \leq i < e$, the limit

$$\lim_{k\to\infty} W_{p^{ke+i}} \quad \text{exists in } \mathbb{Z}_p? \tag{21}$$

If the underlying elliptic curve $E$ has split multiplicative reduction at $p$, so $E(\mathbb{Q}_p) \cong \mathbb{Q}_p^*/q^{\mathbb{Z}}$, then the limit (21) exists and can be expressed in terms of Tate's $p$-adic sigma function ([11, V §3]) and the Teichmüller character. In general, we conjecture that the limit (21) contains interesting $p$-adic information related to the elliptic Teichmüller function $E(\mathbb{Q}_p) \to E(\mathbb{Q}_p)_{\text{tors}}$ and to the Mazur-Tate $p$-adic sigma function [8].

*Proof (of Lemma 6).* The EDS recurrence (1) allows one to compute an entire EDS from its first four terms. More generally, it is possible to generate the subsequence $(W_{dn})_{n\geq 1}$ from the initial four values $W_d, W_{2d}, W_{3d}, W_{4d}$ using the recurrence

$$W_d^2 W_{(n+2)d} W_{(n-2)d} = W_{2d}^2 W_{(n+1)d} W_{(n-1)d} - W_d W_{3d} W_{nd}^2.$$

In particular, the following formulas express $W_{6d}$ and $W_{8d}$ in terms of $W_d, W_{2d}, W_{3d}, W_{4d}$:

$$W_{6d} = W_{3d}\left(\frac{W_{2d}^4 W_{4d}}{W_d^5} - \frac{W_{2d} W_{3d}^3}{W_d^4} - \frac{W_{4d}^2}{W_d W_{2d}}\right) \tag{22}$$

$$W_{8d} = W_{4d}\left(-\frac{2W_{3d}^6}{W_d^6} + \frac{3W_{2d}^3 W_{3d}^3 W_{4d}}{W_d^7} - \frac{W_{3d}^3 W_{4d}^2}{W_d^3 W_{2d}^2} - \frac{W_{2d}^6 W_{4d}^2}{W_d^8}\right) \tag{23}$$

We use induction to prove that $W_{2^k}$ is odd. We are given that $W_1, W_2$, and $W_4$ are odd. Assume now that $W_{2^k}$, $W_{2^{k+1}}$ and $W_{2^{k+2}}$ are odd for some $k \ge 0$. We apply (23) with $d = 2^k$. Since $W_d \equiv W_{2d} \equiv W_{4d} \equiv 1 \pmod 2$ by hypothesis, we can reduce (23) modulo 2 to obtain

$$W_{2^{k+3}} = W_{8d} \equiv 1 \cdot (-2 + 3W_{3d}^3 - W_{3d}^3 - 1) \equiv 1 \pmod 2.$$

Hence $W_{2^{k+3}}$ is odd, which completes the induction proof.

Now consider the map

$$F : \mathbb{N} \longrightarrow \left(\frac{\mathbb{Z}}{2^e\mathbb{Z}}\right)^4, \qquad k \longrightarrow \bigl(W_{2^k}, W_{2\cdot 2^k}, W_{3\cdot 2^k}, W_{2^e\cdot 2^k}\bigr) \bmod 2^e.$$

We observe that the first two coordinates of $F(k+1)$ are simply the second and fourth coordinates of $F(k)$, while the last two coordinates of $F(k+1)$ can be computed from the coordinates of $F(k)$ using the formulas (22) and (23). (Note that we are using the fact that all $W_{2^k}$ are odd, since otherwise we could not simply reduce (22) and (23) modulo $2^e$.)

We have shown that $F(k+1)$ is completely determined by $F(k)$. Since the range of $F$ is a finite set, it must eventually repeat a value, say $F(r+K) = F(K)$ for some $K \ge 0$ and $r \ge 1$. It follows that $F(r+k) = F(k)$ for all $k \ge K$. $\square$

**Theorem 7.** *Let $(W_n)$ be an unbounded nonsingular elliptic divisibility sequence. Then the sequence of absolute values $(|W_n|)$ is not realizable.*

*Proof.* Suppose that $(|W_n|)$ is realizable. Applying Lemma 5 with $n = 2^k$ (i.e., equation (20) with $p = 2$), we see that

$$|W_{2^k}| \equiv |W_{2^{k-1}}| \pmod{2^k} \qquad \text{for all } k \ge 1. \tag{24}$$

In particular, since $W_1 = 1$ is odd, we see that $W_{2^k}$ is odd for all $k$. This allows us to apply Lemma 6, which we do with $e = 2$. Thus we find integers $r, K > 0$ so that

$$W_{2^{r+k}} \equiv W_{2^k} \pmod 4 \qquad \text{for all } k \ge K. \tag{25}$$

On the other hand, (24) certainly implies that

$$|W_{2^{r+k}}| \equiv |W_{2^k}| \pmod 4 \qquad \text{for all } k \ge 1. \tag{26}$$

The two congruences (25) and (26) imply that for each $j$ with $0 \le j < r$, the quantity

$$\operatorname{Sign}(W_{2^{ri+j}}) \text{ is constant for all } i \ge K.$$

However, Theorem 4 tells us that there is an irrational number $\beta \in \mathbb{R}$ with the property that

$$\operatorname{Sign}(W_{2^k}) = (-1)^{\lfloor 2^k\beta \rfloor} \qquad \text{for all } k \ge 1,$$

so the assumption that $(|W_n|)$ is realizable leads to the conclusion that for each $0 \le j < r$, the parity of $\lfloor 2^{ri+j}\beta \rfloor$ is constant for all $i \ge K$. In other words, the parity of $\lfloor 2^k \beta \rfloor$ is eventually periodic. Then an elemenatry argument (see Lemma 8 below) implies that $\beta \in \mathbb{Q}$, contradicting the fact that $\beta$ is irrational. This completes the proof that $(|W_n|)$ is not realizable. $\square$

**Lemma 8.** *Let $\beta \in \mathbb{R}$ and suppose that the parity of $\lfloor 2^k \beta \rfloor$ is eventually periodic, i.e., there are integers $r \ge 1$ and $K$ so that for each $0 \le j < r$, the quantity $\lfloor 2^{ri+j}\beta \rfloor$ is constant for all $i \ge K$. Then $\beta \in \mathbb{Q}$.*

*Proof.* Write the binary expansion of the fractional part of $\beta$ as

$$\beta = \lfloor \beta \rfloor + \sum_{k=1}^{\infty} \frac{b_k}{2^k} \qquad \text{with } b_k \in \{0, 1\}.$$

The parity of $\lfloor 2^k \beta \rfloor$ is simply the coefficient $b_k$, so our assumption says that the sequence of binary coefficients $(b_k)$ is eventually periodic. Hence $\beta$ is rational. $\square$

*Acknowledgements.* The authors would like to thank Graham Everest, Alf van der Poorten, Igor Shparlinski, Thomas Ward and Gary Walsh for helpful disucssions about (elliptic) divisibility sequences.

## References

[1] J.P. Bézivin, A. Pethö, A.J. van der Poorten, A full characterization of divisibility sequences, *Amer. J. of Math.* **112** (1990), 985–1001.

[2] L.K. Durst, The apparition problem for equianharmonic divisibility, Proc. Nat. Acad. Sci. U. S. A. **38** (1952), 330–333.

[3] M. Einsiedler, G. Everest, T. Ward, Primes in elliptic divisibility sequences, *LMS J. Comput. Math.* **4** (2001), 1–13, electronic.

[4] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs 104, AMS, Providence, RI, 2003.

[5] G. Everest, Y. Puri, T. Ward, Integer sequences counting periodic points, *Journal of Integer Sequences* (electronic) **5** (2002), 1-10. (ArXiv math.NT/0204173)

[6] G. Everest, T. Ward, Primes in divisibility sequences, *Cubo Mat. Educ.* **3** (2001), 245–259.

[7] ______ The canonical height of an algebraic point on an elliptic curve, *New York J. Math.* 6 (2000), 331-342, (electronic).

[8] B. Mazur, J. Tate, The $p$-adic sigma function, *Duke Math. J.* **62** (1991), 663–688.

[9] R. Shipsey, Elliptic divisibility sequences, Ph.D. thesis, Goldsmith's College (University of London), 2000.

[10] J.H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.

[11] ______ *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994.

[12] ______ Algebraic divisibility sequences and Vojta's conjecture for exceptional divisors, in preparation.

[13] C.S. Swart, Elliptic divisibility sequences, Ph.D. thesis, Royal Holloway (University of London), 2003.

[14] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics 1239, Springer-Verlag, Berlin, 1987.

[15] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948), 31–74.

[16] M. Ward, The law of repetition of primes in an elliptic divisibility sequence, *Duke Math. J.* **15** (1948), 941–946.

## Appendix A. The elliptic curve associated to an elliptic divisiblity sequence

The material in this appendix is essentially taken from Ward's paper [15]. Let $(W_n)$ be an elliptic divisibility sequence starting

$$W_1 = 1, \quad W_2 = \alpha, \quad W_3 = \beta, \quad W_4 = \alpha\gamma.$$

(Notice that we have built in the divisibility of $W_4$ by $W_2$.) Define quantities

$$\begin{aligned}
A &= 3^3 \cdot \bigl(-\alpha^{16} - 4\gamma\alpha^{12} + \bigl(16\beta^3 - 6\gamma^2\bigr)\alpha^8 + \bigl(8\gamma\beta^3 - 4\gamma^3\bigr)\alpha^4 \\
&\qquad\qquad - \bigl(16\beta^6 + 8\gamma^2\beta^3 + \gamma^4\bigr)\bigr) && (27)\\
B &= 2 \cdot 3^3 \cdot \bigl(\alpha^{24} + 6\gamma\alpha^{20} - \bigl(24\beta^3 - 15\gamma^2\bigr)\alpha^{16} - \bigl(60\gamma\beta^3 - 20\gamma^3\bigr)\alpha^{12} \\
&\qquad\qquad + \bigl(120\beta^6 - 36\gamma^2\beta^3 + 15\gamma^4\bigr)\alpha^8 \\
&\qquad\qquad + \bigl(-48\gamma\beta^6 + 12\gamma^3\beta^3 + 6\gamma^5\bigr)\alpha^4 \\
&\qquad\qquad + \bigl(64\beta^9 + 48\gamma^2\beta^6 + 12\gamma^4\beta^3 + \gamma^6\bigr)\bigr) && (28)\\
x &= 3 \cdot \bigl(\alpha^8 + 2\gamma\alpha^4 + 4\beta^3 + \gamma^2\bigr) && (29)\\
y &= -108\beta^3\alpha^4 && (30)\\
\mathrm{Disc} &= 4A^3 + 27B^2 \\
&= 2^8 \cdot 3^{12} \cdot \beta^9\alpha^8\bigl(\gamma\alpha^{12} + \bigl(-\beta^3 + 3\gamma^2\bigr)\alpha^8 + \bigl(-20\gamma\beta^3 + 3\gamma^3\bigr)\alpha^4 \\
&\qquad\qquad + \bigl(16\beta^6 + 8\gamma^2\beta^3 + \gamma^4\bigr)\bigr) && (31)
\end{aligned}$$

Then the elliptic divisibility sequence $[1, \alpha, \beta, \alpha\gamma, \cdots]$ is associated to the elliptic curve $E$ and rational point $P \in E$ given by the equations

$$E : Y^2 = X^3 + AX + B \qquad \text{and} \qquad P = (x, y) \in E.$$

Up to a substitutation and a linear shift of coordinates, the formulas (27)–(31) for $A$, $B$, $x$, $y$, and Disc may be found in Ward's paper [15] as, respectively, equations (13.6), (13.7), (13.5), (13.1), and (19.3).

Mathematics Department, Box 1917, Brown University, Providence, RI 02912 USA

*E-mail address*: `jhs@math.brown.edu`

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, UK

*E-mail address*: `nelson.stephens@rhul.ac.uk`